Network Protocol Configuration

Table of Contents

Chapter 1 Configuring IP Addressing

1.1 IP Introduction

1.1.1 IP

Internet Protocol (IP) is a protocol in the network to exchange data in the text form. IP has the functions such as addressing, fragmenting, regrouping and multiplexing. Other IP protocols (IP protocol cluster) are based on IP. As a protocol working on the network layer, IP contains addressing information and control information which are used for routing.

Transmission Control Protocol (TCP) is also based on IP. TCP is a connection-oriented protocol which regulates the format of the data and information in data transmission. TCP also gives the method to acknowledge data is successfully reached. TCP allows multiple applications in a system to communicate simultaneously because it can send received data to each of the applications respectively.

The IP addressing, such as Address Resolution Protocol, are to be described in section "Configuring IP Addressing." IP services such as ICMP, HSRP, IP statistics and performance parameters are to be described in "Configuring IP Services."

1.1.2 IP Routing Protocol

Our routing OLT supports multiple IP routing dynamic protocols, which will be described in the introduction of each protocol.

IP routing protocols are divided into two groups: Interior Gateway Routing Protocol (IGRP) and Exterior Gateway Routing Protocol (EGRP). GP3616 Series OLT supports RIP and OSPF. You can configure RIP and OSPF respectively according to your requirements. Our OLT also supports the process that is to configure multiple routing protocols simultaneously, a random number of OSPF processes (if memory can be distributed), a BGP process, a RIP process and a random number of BEIGRP processes. You can run the redistribute command to redistribute the routes of other routing protocols to the database of current routing processes, connecting the routes of multiple protocol processes.

To configure IP dynamic routing protocols, you must first configure relevant processes, make relevant network ports interact with dynamic routing processes, and then designate routing processes to be started up on the ports. To do this, you may check configuration steps in configuration command documents.

(1) Choosing Routing Protocol

It is a complex procedure to choose routing protocol. When you choose the routing protocol, consider the following items:

- Size and complexity of the network
- Whether the length-various network need be supported
- Network traffic
- Safety requirements
- Reliability requirements

- Strategy
- Others

Details of the above items are not described in the section. We just want to remind you that your network requirements must be satisfied when you choose the routing protocols.

(2) IGRP

Interior Gateway Routing Protocol (IGRP) is used for network targets in an autonomous system. All IP IGRPs must be connected with networks when they are started up. Each routing process monitors the update message from other routing devices in the network and broadcasts its routing message in the network at the same time. GP3616 Series OLT supports following internal routable protocols:

RIP

OSPF

(3) EGRP

Exterior Gateway Routing Protocol (EGRP) is used to exchange routing information between different autonomous systems. Neighbors to exchange routes, reachable network and local autonomous system number generally need to be configured. GP3616 Series OLT does not support external routable protocols at present:

1.2 Configuring IP Address Task List

An essential and mandatory requirement for IP configuration is to configure the IP address on the network interface of the routing OLT. Only in this case can the network interface be activated, and the IP address can communicate with other systems. At the same time, you need to confirm the IP network mask.

To configure the IP addressing, you need to finish the following tasks, among which the first task is mandatory and others are optional.

For creating IP addressing in the network, refer to section “IP Addressing Example.”

IP address configuration task list:

- Configuring IP address at the network interface
- Configuring multiple IP addresses at the network interface
- Configuring Address Resolution
- Configuring broadcast packet processing
- Detecting and maintaining IP addressing

1.3 Configuring IP Address

1.3.1 Configuring IP Address at the Network Interface

The IP address determines the destination where the IP message is sent to. Some IP special addresses are reserved and they cannot be used as the host IP address or network address. Table 1 lists the range of IP addresses, reserved IP addresses and available IP addresses.

Type	Address or Range	Status
A	0.0.0.0 1.0.0.0 to 126.0.0.0	Reserved Available

	127.0.0.0	Reserved
B	128.0.0.0 to 191.254.0.0 191.255.0.0	Available Reserved
C	192.0.0.0 192.0.1.0 to 223.255.254 223.255.255.0	Reserved Available Reserved
D	224.0.0.0 to 239.255.255.255	Multicast address
E	240.0.0.0 to 255.255.255.254 255.255.255.255	Reserved Broadcast

The official description of the IP address is in RFC 1166 “Internet Digit”. You can contact the Internet service provider.

An interface has only one primary IP address. Run the following command in interface configuration mode to configure the primary IP address and network mask of the network interface:

Command	Purpose
ip address *ip-address mask*	Configure the main IP address of the interface.

The mask is a part of the IP address, representing the network.

Note:

Our OLT only supports masks which are continuously set from the highest byte according to the network character order.

1.3.2 Configuring Multiple IP Addresses at the Network Interface

Each interface can possess multiple IP addresses, including a primary IP address and multiple subordinate IP addresses. You need to configure the subordinate IP addresses in the following two cases:

If IP addresses in a network segment are insufficient. For example, there are only 254 available IP addresses in a certain logical subnet, however, 300 hosts are needed to connect the physical network. In this case, you can configure the subordinate IP address on the OLT or the server, enabling two logical subnets to use the same physical subnet.

Most of early-stage networks which are based on the layer-2 bridge are not divided into multiple subnets. You can divide the early-stage network into multiple route-based subnets by correctly using the subordinate IP addresses. Through the configured subordinate IP addresses, the routing OLT in the network can know multiple subnets that connect the same physical network.

If two subnets in one network are physically separated by another network In this case, you can take the address of the network as the subordinate IP address. Therefore, two subnets in a logical network that are physically separated, therefore, are logically connected together.

Note:

If you configure a subordinate IP address for a routing OLT in a network segment, you need to do

this for other routing OLT in the same network segment.
Run the following command in interface configuration mode to configure multiple IP addresses on the network interface.

Command	Purpose
ip address *ip-address mask* **secondary**	Configures multiple IP addresses on the network interface.

Note:
When the IP routing protocol is used to send the route update information, subordinate IP addresses may be treated in different ways.
1.3.3 Configuring Address Resolution
IP can realize functions such as IP address resolution control. The following sections show how to configure address resolution:

(1) Creating Address Resolution

An IP device may have two addresses: local address (local network segment or device uniquely identified by LAN) and network address (representing the network where the device is located). The local address is the address of the link layer because the local address is contained in the message header at the link layer, and is read and used by devices at the link layer. The professionals always call it as the MAC address. This is because the MAC sub layer in the link layer is used to process addresses.
For example, if you want your host to communicate with a device on Ethernet, you must know the 48-bit MAC address of the device or the local address of the link layer. The process on how to obtain the local address of the link layer from the IP address is called as Address Resolution Protocol (ARP). The process on how to obtain the IP address from the local address of the link layer is called as Reverse Address Resolution (RARP).
Our system adopts address resolution in two types: ARP and proxy ARP. The ARP and proxy ARP are defined in RFC 860 and 1027 respectively.
ARP is used to map IP addresses to media or MAC address. When the IP address is known, ARP will find the corresponding MAC address. When the MAC address is known, the mapping relationship between IP address and MAC address is saved in ARP cache for rapid access. The IP message is then packaged in the message at the link layer and at last is sent to the network.
Defining a static ARP cache
ARP and other address resolution protocols provide a dynamic mapping between IP address and MAC address. The static ARP cache item is generally not required because most hosts support dynamic address resolution. You can define it in global configuration mode if necessary. The system utilizes the static ARP cache item to translate the 32-bit IP address into a 48-bit MAC address. Additionally, you can specify the routing OLT to respond to the ARP request for other hosts.
You can set the active period for the ARP entries if you do not want the ARP entry to exist permanently. The following two types show how to configure the mapping between the static IP address and the MAC address.

Run one of the following commands in global configuration mode:

Command	Purpose
arp ip-address hardware-address **vlan** vlan-id	Globally maps an IP address to a MAC address in the ARP cache.
arp ip-address hardware-address **vlan** vlan-id **alias**	Specifies the routing OLT to respond to the ARP request of the designated IP address through the MAC address of the routing OLT.

Run the following command in VLAN interface configuration mode:

Command	Purpose
arp timeout *seconds*	Sets the timeout time of the ARP cache item in the ARP cache.
arp dynamic	Enables arp dynamic learning in the interface

Run show interfaces to display the ARP timeout time of the designated interface. Run the show arp to check the content of the ARP cache. Run clear arp-cache to delete all entries in the ARP cache.

Activating proxy ARP

The system uses the proxy ARP (defined by RFC 1027) to obtain the host's MAC address on other networks for the hosts without corresponding routes. For example, when the routing OLT receives an ARP request and finds that the source host and the destination host are not connected to the same interface and all the routes that the routing OLT reaches the destination host are not through the interface that receives the ARP request, it will send a proxy ARP response that contains its address of the link layer. The source host then sends the message to the routing OLT and the OLT forwards it to the destination host. The proxy ARP is activates by default.

To activate the proxy ARP, run the following command in interface configuration mode:

Command	Purpose
ip proxy-arp	Activates the proxy ARP on the interface.

Configuring free ARP function

The OLT can know whether the IP addresses of other devices collide with its IP address by sending free ARP message. The source IP address and the destination IP address contained by free ARP message are both the local address of the OLT. The source MAC address of the message is the local MAC address.

The OLT processes free ARP message by default. When the OLT receives free ARP message from a device and finds that the IP address contained in the message collide with its own IP address, it will return an ARP answer to the device, informing the device that the IP addresses

collide with each other. At the same time, the OLT will inform users by logs that IP addresses collide.

The OLT's function to send free ARP message is disabled by default. Run the following commands to configure the free ARP function on the port of the OLT:

Command	Purpose
arp send-gratuitous	Starts up free ARP message transmission on the interface.
arp send-gratuitous interval *value*	Sets the interval for sending free ARP message on the interface. The default value is 120 seconds.

To set the waiting time of ARP cache resolution, run the following command.

The OLT will create incomplete ARP entry when first resolve arp. The incomplete entry will create complete ARP entry when the opposite end responses correct arp reply packet. At this point, the ARP resolution is finished.

Run following command to set the time to live of the incomplete entry.

Command	Purpose
arp pending-time *seconds*	Sets the waiting time of ARP cache resolution, run the following command: The default value is 15 seconds.

Set the maximum number of incomplete ARP entries.

Command	Purpose
arp max-incomplete *number*	Sets the maximum number of incomplete ARP entries. The default is 0.

To set the maximum retransmissions of the Re-Detect packets, run the following command.

The ARP entries (to be tagged with G), which the routing entry gateway depends on, require being re-detected at their aging so that the promptness and correctness of the hardware subnet routing can be guaranteed. The greater the retransmission times, the more likely to re-detect.

Command	Purpose
arp max-gw-retries *number*	Sets the maximum retransmissions of the Re-Detect packets. The default is 3.

Set re-detection when ARP entry is aging.

By default only ARP depends on routing entry has re-detection when aging. After enable this command, all ARP entries will adopt aging re-detection mechanism.

Command	Purpose
arp retry-allarp	Sets re-detection when the ARP entry is aging.

(2) Mapping Host Name to IP Address

Any IP address can correspond to a host name. The system has saved a mapping (host name to address) cache which can be telneted or pinged.

To designate a mapping from host name to address, run the following commands in global mode:

Command	Purpose
ip host *name address*	Statically maps the host name to the IP address.

1.3.4 Configuring Routing Process

You can configure one or multiple routing protocols according to your actual network requirements. The routing protocol provides information about the network topology. The details about configuring IP routing protocols such as BGP, RIP and OSPF are shown in the following sections.

1.3.5 Configuring Broadcast Packet Process

The destination addresses of the broadcast message are all the hosts on a physical network. The host can identify the broadcast message through special address. Some protocols, including some important Internet protocols, frequently use the broadcast message. One primary task of the IP network administrator is to control the broadcast message. The system supports the directed broadcast, that is, the broadcast of designated network. The system does not support the broadcast of all subnets in a network.

Some early-stage IP's do not adopt the current broadcast address standard. The broadcast address adopted by these IPs is represented completely by the number "0", not "1" completely. The system can simultaneously identify and receive message of the two types.

(1) Allowing Translating from Directed Broadcast to Physical Broadcast

By default, the IP directional broadcast packets will be dropped, rather than being forwarded. Dropping the IP directional broadcast packet is conducive to prevent the routing OLT from attacks of "refusal service".

You can activate the function of forwarding directed IP broadcast on the interface where the directed broadcast is transformed to the physical message. If the forwarding function is activated, all the directed broadcast message of the network that connects the interface will be forwarded to the interface. The message then will be sent as the physical broadcast message.

You can designate an access table to control the forwarding of broadcast message. After the access table is specified, only IP message that the access table allows can be transformed from the directed broadcast to the physical broadcast.

Run the following command in interface configuration mode to activate the forwarding of the directed broadcast.

Command	Purpose
ip directed-broadcast [*access-list-name*]	Allows the translation from the directed broadcast to the physical broadcast on the interface.

(2) Forwarding UDP Broadcast Message

Sometimes, the host uses the UDP broadcast message to determine information about the

address, configuration and name, and so on. If the network where the host is located has no corresponding server to forward the UDP message, the host cannot receive any of the UDP message. To solve the problem, you can do some configuration on the corresponding interface to forward some types of broadcast message to an assistant address. You can configure multiple assistant addresses for an interface.

You can designate a UDP destination port to decide which UDP message is to be forwarded. Currently, the default forwarding destination port of the system is UDP packet of NetBIOS name service (port 137).

Run the following command in interface configuration mode to allow message forwarding and to specify the destination address:

Command	Purpose
ip helper-address *address*	Allows to forward the UDP broadcast message and to specify the destination address.

Run the following command in global configuration mode to specify protocols to be forwarded:

Command	Purpose
ip forward-protocol udp [*port*]	Specifies which interfaces' UDP protocols will be forwarded.

1.3.6 Detecting and Maintaining IP Address

To detect and maintain the network, run the following command:

(1) Clearing Cache, List and Database

Clearing cache, list and database You can clear all content in a cache, list or the database. When you think some content is ineffective, you can clear it.

Run the following command in management mode to clear the cache, list and database:

Command	Purpose
clear arp-cache	Clears the IP ARP cache.

(2) Displaying Statistics Data about System and Network

The system can display designated statistics data, such as IP routing table, cache and database. All such information helps you know the usage of the systematic resources and solve network problems. The system also can display the reachability of the port and the routes that the message takes when the message runs in the network.

All relative operations are listed in the following table. For how to use these commands, refer to Chapter "IP Addressing Commands". Run the following commands in management mode:

Command	Purpose
show arp	Displays content in the ARP table.
show hosts	Displays the cache table about hostname-to-IP mapping.
show ip interface [*type number*]	Displays the state of a port.
ping {**host	address**}	Tests the reachability of the network node.

1.4 IP Addressing Example

The following case shows how to configure the IP address on interfaceVLAN11.

```
interface vlan 11
ip address 202.96.2.3 255.255.255.0
```

Chapter 2 Configuring DHCP

2.1 Overview

Dynamic Host Configuration Protocol (DHCP) is used to provide some network configuration parameters for the hosts on the Internet, which is described in details in RFC 2131. One of the major functions of DHCP is to distribute IPs on an interface. DHCP supports the following three IP distribution mechanism:

Automatic distribution

The DHCP server automatically distributes a permanent IP address to a client.

Dynamic distribution

The DHCP server distributes an IP address for a client to use for a certain period of time or until the client does not use it.

Manual distribution

The administrator of the DHCP server manually specifies an IP address and through the DHCP protocol sends it to the client.

2.1.1 DHCP Application

DHCP can be applied at the following cases: You can distribute IP address, network segment and related sources (such as relevant gateway) to an Ethernet interface by configuring the DHCP client.

When an OLT that can access DHCP connects multiple hosts, the OLT can obtain an IP address from the DHCP server through the DHCP relay and then distribute the address to the hosts.

2.1.2 Advantages of DHCP

In current software version, the DHCP client or the DHCP client on the Ethernet interface is supported. DHCP has the following strong points:

Fastening the settings;

Reducing configuration errors;

Controlling IP addresses of some device ports through the DHCP server

2.1.3 DHCP Terms

DHCP is based on the server/client mode. So the DHCP server and the DHCP client must exist at the same time:

DHCP-Server

It is a device to distribute and recycle the DHCP-related sources such as IP addresses and lease time.

DHCP-Client

It is a device to obtain information from the DHCP server for devices of the local system to use, such as IP address information.

In a word, there exists lease time during the process of dynamic DHCP distribution:

Lease time – it means the effective period of an IP, which starts from the distribution. After the lease time, the DHCP server withdraws the IP. To continue to use this IP, the DHCP client needs to apply it again.

2.2 Configuring DHCP Client

2.2.1 Configuration Task List of DHCP Client

- Obtaining an IP address
- Specifying an address for DHCP server
- Configuring DHCP parameters
- Monitoring DHCP

2.2.2 DHCP Client Configuration Tasks

(1) Obtaining an IP address

Run the following command on the VLAN interface to obtain an IP address through the DHCP protocol for an interface.

Command	Purpose
ip address dhcp	Sets the IP address of an Ethernet interface through DHCP.

(2) Specifying an Address for DHCP Server

If knowing the addresses of some DHCP servers, you can specify these servers' addresses on OLT so as to reduce the time of protocol processing. You can run the following command in global mode:

Command	Purpose
ip dhcp-server *ip-address*	Specifies the IP address of the DHCP server.

The command is optional when you perform operations to "obtain an IP address".

(3) Configuring DHCP Parameters

To adjust the parameters of DHCP communication according to actual requirements, run the following commands in global mode:

Command	Purpose
ip dhcp client minlease *seconds*	Specifies the acceptable minimum lease time.
ip dhcp client retransmit *count*	Specifies the retransmission times for DHCP packet.
ip dhcp client select *seconds*	Specifies the interval for SELECT.
ip dhcp client class_identifier *WORD*	Specifies the classification code of the provider.
ip dhcp client client_identifier hrd_ether	Specifies the client ID as the Ethernet type
ip dhcp client timeout_shut	Specifies client timeout shutdown of the interface
ip dhcp client retry_interval *<1-1440>*	Sets the re-transmission time.
ip dhcp client bootfileaddmac	Enables DHCP file name to add MAC address

	of the client
ip dhcp client tftpdownload	Enables TFTP download function

The command is optional when you perform operations to "obtain an IP address".

(4) Monitoring DHCP

To browse related information of the DHCP server, which is discovered by OLT currently, run the following command in EXEC mode:

Command	Purpose
show dhcp server	Displays related information about the DHCP server, which is known by OLT.

To browse which IP address is currently used by OLT, run the following command in EXEC mode:

Command	Purpose
show dhcp lease	Displays IP resources, which are currently used by the OLT, and related information.

Additionally, if you use DHCP to distribute an IP for an Ethernet interface, you can also run show interface to browse whether the IP address required by the Ethernet interface is successfully acquired.

2.2.3 DHCP Client Configuration Example

DHCP Client configuration example is shown below:

(1) Obtaining an IP Address

The following example shows interface vlan11 obtains an IP address through DHCP.

!

interface vlan 11

ip address dhcp

2.3 Configuring DHCP Server

2.3.1 DHCP Server Configuration Tasks

- Enabling DHCP server
- Disabling DHCP server
- Configuring ICMP detection parameter
- Configuring database storage parameter
- Configuring the address pool of DHCP server
- Configuring the parameter for the address pool of DHCP server
- Monitoring DHCP server
- Clearing information about DHCP server

2.3.2 Setting the Address Pool of DHCP Server

(1) Enabling DHCP Server

To enable the DHCP server and distribute IP addresses for DHCP client, run the following commands in global mode (thereupon, the DHCP server also supports the relay operation; As to those IPs that the DHCP server cannot distribute, the interface on which IP helper-address is

configured will forward the DHCP request)

Command	Purpose
ip dhcpd enable	Enables DHCP server

(2) Disabling DHCP Server Service

To disable DHCP server and stop distributing parameters such as IP address parameter for the DHCP client, run the following command in global configuration mode:

Command	Purpose
no ip dhcpd enable	Disables DHCP server

(3) Configuring ICMP Detection Parameter

You can adjust the parameters of ICMP packet transmission according to actual requirements when the DHCP server is checking addresses.

To set the number of ICMP packets to be sent, run the following command in global mode:

Command	Purpose
ip dhcpd ping packets *pkgs*	Sets how many ICMP packets to be sent during address checkup.

To set the timeout time of ICMP response, run the following command in global mode:

Command	Purpose
ip dhcpd ping timeout *timeout*	Sets the timeout time of ICMP response.

(4) Setting a Parameter to Clear the “Abandoned” Mark

To set the interval of clearing the “Abandoned” mark, run the following command in global mode:

Command	Purpose
ip dhcpd abandon-time *time*	Sets the interval of clearing the “Abandoned” mark.

(5) Configuring Database Storage Parameter

To set the interval of storing the address distribution information to the agent database, run the following command in global mode:

Command	Purpose
ip dhcpd write-time *time*	Sets the interval for storing the address distribution information to the agent database.

(6) Configuring DHCP File Domain

Run the following command in the global configuration mode:

Command	Purpose

ip dhcpd bootfile-name *word*	The command is used to configure DHCP file domain.

(7) Configuring DHCP Enabling File Name Option

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd bootfile-option	The following command is used to configure DHCP enabling file name option.

(8) Configuring DHCP Supporting BOOTP Client

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd bootp [auto-bind]	The command is used to configure DHCP supporting BOOTP client. auto-bind means to allow BOOTP client distributing auto binding address.

(9) Configuring DHCP Database Server Address

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd database-agent *ip-address*	Configures DHCP database server address, run the following command. If this address is not set, the address distribution information will be saved to the flash. Note: Before the address distribution information is saved, PC should enable the TFTP server and also PC and the DHCP server should connect correctly.

(10) Configuring DHCP Database File Name

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd database-file *word* [**time-stamp**]	Configures the DHCP database file name, run the following command. Word means database file name

	Time-stamp means file name addition time stamp

(11) Saving the Change of Cache Entry in Time to the Data Base File

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd database-realtime	Saves the change of cache entry in time to the data base file, run the following command.

(12) Configuring DHCP Optional Server Host Name

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd server-name *name*	Configures DHCP optional server host name.

(13) Enabling DHCP TFTP Server Name Option

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd sname-option	Enables DHCP TFTP server name option.

(14) Configuring Relevant Parameters of DHCP Snooping

The command can be used to enable the ARP map protection. When this command is set, the DHCP server will establish an ARP map between the MAC address and distributed IP address of the DHCP client, and then protect this ARP map. Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd snooping arp	Configures the parameters of DHCP snooping.

(15) Forwarding STB DHCP Data Packet

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd relay-STB	Enables STB DHCP data packet.

(16) Compulsorily Enabling DHCP TFTP Server Name Option and DHCP Enabling File Name Option

To compulsorily enable DHCP TFTP server name option (option:66) and DHCP enabling file name option (option: 67). Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd sname-bootfile-option-force	Compulsorily enables DHCP TFTP server name option (option:66) and DHCP enabling file name option (option: 67).

(17) Configuring Address Pool of DHCP Server

To add the address pool of DHCP server, run the following command in global mode:

Command	Purpose
ip dhcpd pool *name*	Adds the address pool of DHCP server and enters the configuration mode of the DHCP address pool.

(18) Configuring Relevant Parameters for the Address Pool of DHCP Server

In the configuration mode of DHCP address pool, you can run the following commands to set related parameters.

To set the network address of the address pool of automatic distribution, run the following command:

Command	Purpose
network *ip-addr netsubnet*	Sets the network address of the address pool of automatic distribution.

To set the address range of automatic distribution, run the following command:

Command	Purpose
range *low-addr high-addr*	Sets the address range of automatic distribution.

To set the default route, which is distributed by the client, run the following command:

Command	Purpose
default-router *ip-addr …*	Sets the default route that is distributed to the client.

To set the address of DNS server, which is distributed to the client, run the following command:

Command	Purpose
dns-server *ip-addr …*	Sets the address of DNS server, which is distributed to the client.

To set a domain name, which is distributed to the client, run the following command:

Command	Purpose
domain-name *name*	Sets a domain name, which is distributed to the client.

To set the time limitation of the address, which is distributed to the client, run the following command:

Command	Purpose
lease {*days* [*hours*][*minutes*] | *infinite* }	Sets the time limitation of the address, which is distributed to the client.

To set the address of the netbios name server, which is distributed to the client, run the following command:

Command	Purpose
netbios-name-server *ip-addr…*	Sets the address of the netbios name server, which is distributed to the client.

You can run the following command to reject to distribute the IP address to the host whose MAC address is hardware-address.

Command	Purpose
hw-access deny hardware-address	Reject to distribute IP addresses to the host whose MAC address is hardware-address.

(19) Monitoring DHCP Server

To browse the current address distribution information of DHCP server, run the following command in EXEC mode:

Command	Purpose
show ip dhcpd binding	Displays the current address distribution information of DHCP server.

To browse the current packet statistics of DHCP server, run the following command in EXEC mode:

Command	Purpose
show ip dhcpd statistic	Displays the current packet statistics of DHCP server.

To browse the current database server address of DHCP server, run the following command in EXEC mode:

Command	Purpose
show ip dhcpd database-agent	Displays the current address distribution information of DHCP server.

To check the current address pool information of DHCP Server, run the following command in EXEC mode.

Command	Purpose
show ip dhcpd pool	Displays the current address pool information of DHCP server.

(20) Clearing Information about DHCP Server

To delete the current address distribution information of DHCP server, run the following command in EXEC mode:

Command	Purpose
clear ip dhcpd binding {[*ip-addr*]&<0-10>|*}	Deletes the specified address distribution information.

To delete the current packet statistics of DHCP server, run the following command in EXEC mode:

Command	Purpose
clear ip dhcpd statistic	Deletes the current packet statistics of DHCP server.

To delete the current address which has abandoned or disabled by DHCP Server address pool, run the following command in EXEC mode.

Command	Purpose
clear ip dhcpd abandoned	Deletes the current address which has abandoned or disabled by DHCP Server address pool.

2.3.3 DHCP Server Configuration Example

In the following example, the timeout time of the ICMP detection packet is set to 200ms; Address pool 1 is configured and the DHCP server is enabled.

```
ip dhcpd ping timeout 2
ip dhcpd pool 1
 network 192.168.20.0 255.255.255.0
 range 192.168.20.211 192.168.20.215
 domain-name my315
 default-router 192.168.20.1
 dns-server 192.168.1.3 61.2.2.10
```

```
 netbios-name-server 192.168.20.1
 lease 1 12 0
!
ip dhcpd enable
```

2.4 Configuring DHCP Relay

2.4.1 Configuration Task List of DHCP Relay

Enabling DHCP relay

Disabling DHCP relay

Setting the parameters of DHCP relay

2.4.2 DHCP Relay Configuration Tasks

(1) Enabling DHCP Relay

If you want to enable DHCP Relay on OLT, please enable DHCP server first. For details, please refer to section “Enabling the DHCP Server.”

(2) Disabling DHCP Relay

If you want to disable DHCP Relay on OLT, please disable the DHCP server first. For details, please refer to section “Disabling the DHCP Server.”

(3) Setting the Parameters of DHCP Relay

You can modify the destination address of DHCP relay according to requirements. The relay function of the DHCP packet is same in the mechanism of “Forwarding the UDP broadcast packet”. You can refer to the command, ip forward-protocol udp.

2.4.3 DHCP Relay Configuration Example

In the following example, the DHCP relay is enabled, the DHCP-request packet that is received from vlan 1 will be relayed to 10.1.1.1 and at the same time the DHCP-relay packet that arrives 192.168.20.1 will be retransmitted out from VLAN1.

```
interface vlan 1
  ip address 192.168.20.1 255.255.255.0
  ip help-address 10.1.1.1
!
ip dhcpd enable
```

Chapter 3 IP Service Configuration

The section is to describe how to configure optional IP service. For the details of the IP service commands, refer to section “IP Service Commands”.

3.1 Configuring IP Service

Optional IP service configuration tasks are listed as follows:

- Managing IP connection
- Configuring performance parameters
- Configuring default gateway
- Detecting and Maintaining IP Network

The above operations are not mandatory. You can perform the operations according to your requirements.

3.1.1 Managing IP Connection

The IP protocol provides a series of services to control and manage IP connections. Most of these services are provided by ICMP. The ICMP message is sent to the host or other routing OLT when the routing OLT or the access server detects faults in the IP message header. ICMP is mainly defined in RFC 792.

Perform the following different operations according to different IP connection conditions:

(1) Sending ICMP Unreachable Message

If the system receives a message and cannot send it to the destination, such as no routes, the system will send an ICMP-unreachable message to the source host. The function of the system is enabled by default.

If the function is disabled, you can run the following command in VLAN interface configuration mode to enable the function.

Command	Purpose
ip unreachables	Enable the function to send an ICMP-unreachable message.

(2) Sending ICMP Redirection Message

Sometimes the host selects an unfavorable route. After a routing OLT on the route receives a message from the host, it is to check the routing table and then forward the message through the message-receiving interface to another OLT that is in the same network segment as the host. In this case, the OLT notifies the source host of directly sending the message with the destination to another OLT without winding itself. The redirection message requires the source host to discard the original route and take more direct route suggested in the message. Many host’s operating system adds a host route to its routing table. However, the routing OLT is more willing to trust information obtained through the routing protocol. Therefore, the OLT will not add the host route according to the information.

The function is enabled by default. However, if a hot standby OLT protocol is configured on an interface, IPv6 redirection is automatically closed. If the hot standby OLT protocol is canceled, this

function will not automatically opened.

To enable the function, run the following command in VLAN interface configuration mode to forward ICMP re-directional packets:

Command	Purpose
ip redirects	Permit sending the ICMP redirection message.

(3) Sending ICMP Mask Response Message

Sometimes the host must know the network mask. To get the information, the host can send the ICMP mask request message. If the routing OLT can confirm the mask of the host, it will respond with the ICMP mask response message. By default, the routing OLT can send the ICMP mask response message.

To send the ICMP mask request message, run the following command in VLAN interface configuration mode:

Command	Purpose
ip mask-reply	Send the ICMP mask reply message.

(4) Supporting Route MTU Detection

The system supports the IP route MTU detection mechanism defined by RFC 1191. The IP route MTU detection mechanism enables the host to dynamically find and adjust to the maximum transmission unit (MTU) of different routes. Sometimes the routing OLT detects that the received IP message length is larger than the MTU set on the message forwarding interface. The IP message needs to be segmented, but the “unsegmented” bit of the IP message is reset. The message, therefore, cannot be segmented. The message has to be dropped. In this case, the routing OLT sends the ICMP message to notify the source host of the reason of failed forwarding, and the MTU on the forwarding interface. The source host then reduces the length of the message sent to the destination to adjust to the minimum MTU of the route.

If a link in the route is disconnected, the message is to take other routes. Its minimum MTU may be different from the original route. The routing OLT then notifies the source host of the MTU of the new route. The IP message should be packaged with the minimum MTU of the route as much as possible. In this way, the segmentation is avoided and fewer message is sent, improving the communication efficiency.

Relevant hosts must support the IP route MTU detection. They then can adjust the length of IP message according to the MTU value notified by the routing OLT, preventing segmentation during the forwarding process.

(5) Setting IP Maximum Transmission Unit (MTU)

All interfaces have a default IP maximum transmission unit (MTU), that is, the transmissible maximum IP message length. If the IP message length exceeds MTU, the routing OLT segments the message.

Changing the MTU value of the interface is to affect the IP MTU value. If IP MTU equals to MTU, IP MTU will automatically adjust itself to be the same as new MTU as MTU changes. The change of IP MTU, however, does not affect MTU. IP MTU cannot be bigger than MTU configured on the current interface. Only when all devices connecting the same physical media must have the same

MTU protocol can normal communication be created.

To set IP MTU on special interface, run the following command in interface configuration mode:

Command	Purpose
ip mtu *bytes*	Sets IP MTU of the interface.

(6) Authorizing IP Source Route

The routing OLT checks the IP header of every message. The routing OLT supports the IP header options defined by RFC 791: strict source route, relax source route, record route and time stamp. If the OLT detects that an option is incorrectly selected, it will send message about the ICMP parameter problem to the source host and drop the message. If problems occur in the source route, the routing OLT will send ICMP unreachable message (source route fails) to the source host.

IP permits the source host to specify the route of the IP network for the message. The specified route is called as the source route. You can specify it by selecting the source route in the IP header option. The routing OLT has to forward the IP message according to the option, or drop the message according to security requirements. The routing OLT then sends ICMP unreachable message to the source host. OLT supports the source route by default.

If the IP source route is disabled, run the following command in global configuration mode to authorize the IP source route:

Command	Purpose
ip source-route	Authorizes IP source route.

(7) Allowing IP Fast Exchange

IP fast exchange uses the route cache to forward the IP message. Before the OLT forwards message to a certain destination, its system will check the routing table and then forward the message according to a route. The selected route will be stored in the routing cache of the system software. If latter message will be sent to the same host, the OLT will forward latter message according to the route stored in the routing cache. Each time message is forwarded, the value of hit times of the corresponding route item is increasing by 1. When the hit times is equal to the set value, the software routing cache will be stored in the hardware routing cache. The following message to the same host will be forwarded directly by the hardware. If the cache is not used for a period of time, it will be deleted. If the software/hardware cache items reach the upper limitation, new destination hosts are not stored in the cache any more. This OLT series can hold 2074 hardware cache items and 1024 software cache items.

To configure the hit times required when the software cache items are stored to the hardware cache, run the following command in global configuration.

Command	Purpose
ip route-cache hit-numbers *hitnumber*	When the hit times of the routing item in the software cache reaches the value of the parameter hitnumber, the

	routing item in the software cache will be stored as a routing item in the hardware cache.

The command can be enabled in global configuration mode. In case the next hop of the route of the indirectly connected host is same as that of a subnet route, the command will be used to decide whether to delete the hardware route of a host.

Command	Purpose
ip route-cache age-exf	Deletes the indirectly connected hardware route of a host whose next hop is the same with the hardware subnet route next hop.
no ip route-cache age-exf	Saves the indirectly connected hardware route of a host whose next hop is the same with the hardware subnet route next hop.

To set the delay of the route cache, which is caused by ARP change, run the following command in global mode:

Command	Purpose
ip route-cache age-delay *age-delay*	When arp changes, delete all hardware route cache in a delay (related to age-delay).

To set the lifetime of the entries in the software cache, run the following command in global mode:

Command	Purpose
ip route-cache softcache-alive-time *milliseconds*	Deletes the software route cache after milliseconds.

To set the operation time index of the software cache, run the following command in global mode:

Command	Purpose
ip route-cache software-index *ticks*	The bigger the ticks, the faster the OLT can age the invalid software route cache.

To set the operation time index of the hardware route cache, run the following command in global mode:

Command	Purpose
ip route-cache hardware-index *ticks*	The bigger the ticks, the faster the OLT can add the hardware route cache.

To set the lifetime of the hardware route cache, run the following command in global mode:

Command	Purpose
ip route-cache-aging-time *seconds*	Sets the lifetime of the OLT hardware route cache.

To enable the route cache add to the hardware table, run the following command in the global configuration mode:

Command	Purpose
ip route-cache cache-pbr	Adds the route cache which searches the route by the route policy to the hardware table.

(8) Supporting IP Fast Exchange on the Same Interface

You can enable the OLT to support IP fast exchange by making the receiving interface the same as the transmitting interface. Generally, it is recommended not to enable the function because it conflicts with the redirection function of the router.

Run the following command in the VLAN interface configuration mode to allow IP routing cache in the same interface:

Command	Purpose
ip route-cache *same-interface*	Allows IP message with the same receiving/transmitting interfaces to be stored in the routing cache.

3.1.2 Configuring Performance Parameters

Run the following command to adjust IP performance.

(1) Setting the Wait Time for TCP Connection

When the OLT triggers the TCP connection and if the TCP connection is not established in the designated wait time, the OLT views that the connection fails and then sends the result to the upper-layer program. The default value of the system is 75 seconds. The previous configuration has no impact on TCP connections that the OLT forwards. It only affects TCP connections that are created by the OLT itself.

Run the following command in global configuration mode to set the wait time for TCP connections:

Command	Purpose
ip tcp synwait-time *seconds*	Sets the wait time for TCP connection.

(2) Setting the Size of TCP Windows

The default size of TCP windows is 2000 byte. Run the following command in global configuration mode to change the default window size:

Command	Purpose
ip tcp window-size *bytes*	Sets the size of TCP windows.

3.1.3 Detecting and Maintaining IP Network

To detect and maintain the network, run the following command:

(1) Clearing Cache, List and Database

You can clear all content in a cache, list or database. All incorrect data in a cache, list or database need be cleared.

Run the following command to clear incorrect data:

Command	Purpose
clear tcp statistics	Clears the statistics data about TCP

(2) Clearing TCP Connection

To disconnect a TCP connection, run the following command:

Command	Purpose
clear tcp {**local** *host-name port* **remote** *host-name port* | **tcb** *address*}	Clears the designated TCP connection. TCB refers to TCP control block.

(3) Displaying Statistics Data about System and Network

The system can display the content in the cache, list and database. These statistics data can help you know the usage of systematic sources and solve network problems.

The command can be used in other modes except the user mode. For details, refer to “IP Service Command”.

Command	Purpose
show ip access-lists *name*	Displays the content of one or all access lists.
show ip cache [*prefix mask* | **software** | **hardware | vlan** *number* | **summary**]	Displays the routing cache that is used for fast IP message exchange.
show ip sockets	Displays all socket information of OLT.
show ip traffic	Displays IP protocol statistics data
show tcp	Displays all TCP connection status information
show tcp brief	Briefly displays information about TCP connection states.
show tcp statistics	Displays the statistics data about TCP
show tcp tcb *address*	Displays information about the designated TCP connection state.

(4) Displaying Debug Information

When problem occurs on the network, you can run debug to display the debugging information.

Run the following command in EXEC mode. For details, refer to “IP Service Command”.

Command	Purpose
debug arp	Displays the interaction information about ARP.
debug ip icmp	Displays the interaction information about ICMP.
debug ip raw	Displays the information about received/transmitted

	Internet IP message.
debug ip packet	Displays the interaction information about IP.
debug ip tcp packet	Displays the interaction information about TCP.
debug ip tcp transactions	Displays the interaction information about TCP.
debug ip udp	Displays the interaction information about UDP.

3.2 Configuring Access List

3.2.1 Filtering IP Packet

Filtering message helps control the movement of packet in the network. The control can limit network transmission and network usage through a certain user or device. To make packets valid or invalid through the crossly designated interface, our routing OLT provides the access list. The access list can be used in the following modes:

- Controlling packet transmission on the interface
- Controlling virtual terminal line access
- Limiting route update content

The section describes how to create IP access lists and how to use them.

The IP access list is an orderly set of the permit/forbid conditions for applying IP addresses. The ROS software of our OLT tests the addresses one by one in ACL. The first match determines whether the ROS accepts or declines the address. After the first match, the ROS software terminates the match regulations. The order of the conditions is, therefore, important. If no regulations match, the address is declined.

Use the access list by following steps:

(1) Create the access list by designating the access list name and conditions.

(2) Apply the access list to the interface.

3.2.2 Creating Standard and Extensible IP Access List

Use a character string to create an IP access list.

Note:

The standard access list and the extensible access list cannot have the same name.

Run the following command in global configuration mode to create a standard access list:

Command	Purpose
ip access-list standard *name*	Use a name to define a standard access list.
deny [reverse-mask] {*source [source-mask]* | **any**}[**log**][**location**] or **permit [reverse-mask]** {*source [source-mask]* | **any**}[**log**][**location**]	Designate one or multiple permit/deny conditions in standard access list configuration mode. The previous setting decides whether the packet is approved or disapproved.
Exit	Log out from the access list configuration mode.

Run the following command in global configuration mode to create an extensible access list.

Command	Purpose
ip access-list extended *name*	Use a name to define an extensible IP access list.
{deny|permit} [reverse-mask] protocol source source-mask destination destination-mask **[precedence** precedence**] [tos** tos**] [log] [offset-zero] [offset-not-zero] [time-range** rangename**] [totallen {eq | gt | lt}** totallen**] [ttl {eq | gt | lt}** ttl**] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment] [location][dest-portrange][established]**	Designate one or multiple permit/deny conditions in extensible access list configuration mode. The previous setting decides whether the packet is approved or disapproved. precedence means the priority of the IP packet; TOS means Type of Service; offset-zero / offset-not-zero means whether IP packet Fragment offset is 0; is-fragment / not-fragment means whether IP packet is fragmented; donotfragement-notset / donotfragement-set means whether IP packet non-allowed is set; totallen means the total length of the packet; timer-rage means the time range of conditions being effective; ttl means IP packet Time To Live; dest-portrange means the range of destination port; established means established connection
Exit	Log out from the access list configuration mode.

After the access list is originally created, any part that is added later can be put at the end of the list. That is to say, you cannot add the command line to the designated access list. However, you can run no permit and no deny to delete items from the access list.

Note:

When you create the access list, the end of the access list includes the implicit deny sentence by default. If the mask is omitted in the relative IP host address access list, 255.255.255.255 is supposed to be the mask.

When ip acl is applied on the ONU interface, the device does not support configuration of larger, smaller and not equal to L4 port. In other words, L4 port can only be a fixed value.

After the access list is created, the access list must be applied on the route or interface. For details, refer to the following section “Applying the Access List to the Interface”.

3.2.3 Applying the Access List to the Routing Interface

After the access list is created, you can apply it to the routing interface including ingress and egress.

Run the following command in VLAN interface configuration mode.

Command	Purpose
{ip|ipv6} access-group *name* {**in | out**}	Applies the access list to the interface.

The access control list can be used on the incoming or outgoing interface. After a packet is received, the source address of the packet will be checked according to the standard egress interface access control list. For the expanded access control list, the OLT also checks the objective address. If the access control list permits the destination address, the system will continue handling the packet. However, if the access control list forbids the destination address, the system will drop the packet and then returns an ICMP unreachable packet.

For the standard access list of the out interfaces, after a packet is received or routed to the control interface, the software checks the source address of the packet according to the access list. For the expanded access control list, the OLT will also check the access control list at the receiver terminal. If the access list permits the address, the software will send the packet. If the access list does not permit the address, the software drops the packet and returns an ICMP unreachable message.

If the designated access control list does not exist, all packets are allowed to pass through.

3.2.4 Applying the Access List to the Global Mode

After the access list is created, you can apply it to the routing interface in the global configuration mode including ingress and egress.

Run the following command in global mode:

Command	Purpose
[no] {ip|ipv6} access-group *name* **[egress | vlan {**word **| add** word **| remove** word**]**	Applies the established ip access list to an interface or cancels it on the interface in the global configuration mode. name Name of the IP access control list egress The access list is applied in egress. Vlan The access list is applied in ingress. Word vlan range table Add add vlan range table Remove delete vlan range table

If the designated access control list does not exist, all packets are allowed to pass through.

3.2.5 Applying the Access List to the Physical Interface

After the access list is created, you can apply it to the routing interface including ingress and egress.

Run the following command in physical interface configuration mode.

Command	Purpose
[no] {ip|ipv6} access-group *name* **[egress]**	Applies the established ip access list to an interface or cancels it on the interface in the global configuration mode, run the following command: name Name of the IP access control list egress Applies access list on the egress direction. The default is the ingress direction.

If the designated access control list does not exist, all packets are allowed to pass through.

3.2.6 Extensible Access List Example

In the following example, the first line allows any new TCP to connect the destination port after port 1023. The second line allows any new TCP to connect the SMTP port of host 130.2.1.2.

```
ip access-list extended aaa
permit tcp any 130.2.0.0 255.255.0.0 gt 1023
permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface vlan 10
ip access-group aaa in
```

Another example to apply the extensible access list is given. Suppose a network connects the Internet, you expect any host in the Ethernet can create TCP connection with the host in the Internet. However, you expect the host in the Internet cannot create TCP connection with the host in the Ethernet unless it connects the SMTP port of the mail host.

SMTP connects with TCP port in one end and the arbitrary port number in the other end. During the connection period, the same two port numbers are used. The mail packet from the Internet has a destination port, that is, port 25. The outgoing packet has a contrary port number. In fact, the security system behind the routing OLT always receives mails from port 25. That is the exact reason why the incoming service and the outgoing service can be uniquely controlled. The access list can be configured as the outgoing service or the incoming service.

In the following example, the Ethernet is a B-type network with the address 130.20.0.0. The address of the mail host is 130.20.1.2. The keyword established is only used for the TCP protocol, meaning a connection is created. If TCP data has the ACK or RST digit to be set, the match occurs, meaning that the packet belongs to an existing connection.

```
ip access-list aaa
permit tcp any 130.20.0.0 255.255.0.0 established
permit tcp any 130.20.1.2 255.255.255.255 eq 25
interface vlan 10
ip access-group aaa in
```